А К А Д Е М И Я   Н А У К   С С С Р
СИБИРСКОЕ ОТДЕЛЕНИЕ

Ученый совет Института математики по присуждению
ученых степеней

Л.А.ЛЕВИН

НЕКОТОРЫЕ ТЕОРЕМЫ ОБ АЛГОРИТМИЧЕСКОМ ПОДХОДЕ К ТЕОРИИ ВЕРОЯТНОСТЕЙ И ТЕОРИИ ИНФОРМАЦИИ

А в т о р е ф е р а т
диссертации на соискание ученой степени
кандидата физико-математических наук

(Диссертация на русском языке)

01.007 - математическая логика и теория алгоритмов

Новосибирск
1971

А К А Д Е М И Я   Н А У К   С С С Р
СИБИРСКОЕ ОТДЕЛЕНИЕ

Ученый совет Института математики по присуждению
ученых степеней

г.Новосибирск, 90   Тел. 65-05-63

"__"____________ 1971 г.

Ученый совет Института математики Сибирского отделения Академии наук СССР по присуждению ученых степеней направляет Вам для ознакомления автореферат диссертации Л.А.Левина "Некоторые теоремы об алгоритмическом подходе к теории вероятностей и теории информации", представленной на соискание ученой степени кандидата физико-математических наук.

Заверенный учреждением отзыв об автореферате диссертации просим направить в адрес Совета в 2-х экземплярах.

О дне и времени защиты будет объявлено за 10 дней до защиты в газетах "Вечерний Новосибирск" или "Советская Сибирь".

Ученый секретарь Совета
доктор физико-математических наук
профессор   (Д.М.Смирнов).

А К А Д Е М И Я   Н А У К   С С С Р
СИБИРСКОЕ ОТДЕЛЕНИЕ
Ученый совет Института математики по присуждению
ученых степеней

Л.А.ЛЕВИН

НЕКОТОРЫЕ ТЕОРЕМЫ ОБ АЛГОРИТМИЧЕСКОМ ПОДХОДЕ К ТЕОРИИ ВЕРОЯТНОСТЕЙ И ТЕОРИИ ИНФОРМАЦИИ

А в т о р е ф е р а т
диссертации на соискание ученой степени
кандидата физико-математических наук

(Диссертация на русском языке)

01.007 - математическая логика и теория алгоритмов

Новосибирск
1971

Диссертация выполнена
в Московском государственном университете

Научный руководитель -
академик Колмогоров А.Н.

Официальные оппоненты:

доктор физико-математических наук Трахтенброт Б.А.
кандидат физико-математических наук Барздинь Я.М.

Ведущая организация -
Математический институт АН СССР им. Стеклова
(отдел математической логики)

Проблематика, которой посвящена настоящая диссертация, возникла в 1964 году с определения А.Н.Колмогоровым понятия сложности конструктивного объекта (близкие понятия независимо были рассмотрены А.А.Марковым и Р.Дж.Солომоновым). Сложностью слова x по алгоритму $\mathcal{A}$ А.Н.Колмогоров называл минимальную длину двоичного слова p, кодирующего x (т.е.такого, что $\mathcal{A}(p) = x$). Определенная таким образом величина сильно зависит от вида алгоритма $\mathcal{A}$, и центральным результатом, заложившим основы дальнейших исследований,явилась теорема, установленная независимо А.Н.Колмогоровым и (в несколько иных терминах) Р.Дж.Соломоновым. Она утверждает существование оптимального алгоритма $\mathcal{B}$, дающего наименьшее по сравнению с любым другим алгоритмом $\mathcal{A}$ значение сложности с точностью до аддитивной константы $c_{\mathcal{A}}$ (не зависящей от x). Сложность слова x по произвольному оптимальному алгоритму является уже достаточно инвариантной величиной и фундаментальной характеристикой рассматриваемых объектов. Эта величина нашла много применений и породила круг вопросов, который быстро превратился в довольно развитую теорию (см., например, обзорную работу [6]).

В процессе развития этой теории оказалось полезным вве-

сти некоторые другие величины, аналогичные сложности (хотя и не совпадающие с ней).

Одной из наиболее интересных ветвей этого направления оказался алгоритмический подход к основаниям теории информации и теории вероятностей. Этот подход был основан работами А.Н.Колмогорова и затем развит в работах П.Мартин-Лефа, П.К. Шнорра, В.Н.Агафонова и других. Другой интересной вётвью оказалось изучение вопроса сложности разрешения алгоритмических проблем, предпринятое в работах А.А.Маркова, Я.М.Барздиня, М.И.Кановича, Н.В.Петри, Д.Ловеланда и других. Эти работы приведены в библиографии.

Вся вышеописанная проблематика обычно объединяется под названием "сложность алгоритмов", в отличие от более старой проблематики, касающейся "сложности вычислений". Связь между ними изучена еще довольно плохо.

Настоящая диссертация посвящена вопросам "сложности алгоритмов" и алгоритмическому подходу к основаниям теории информации и теории вероятностей. Она состоит из трех глав.

В первой главе, названной "Введение" приводится ряд результатов, сопоставляющих друг с другом различные виды сложностей, вычислимые мажоранты сложностей, произвольные алгоритмически инвариантные функции и т.п. Наиболее важными в этой главе являются результаты, строящие общий подход к разным видам сложностей. Все они (например, сложность $K(x)$, сложность разрешения $KR(x)$, условная сложность, логарифм априорной вероятности и др.) являются различными случаями общей конструкции V-мажорант, которые изучаются в теоремах I-4. В частности, показывается, какую особую роль играет введенная автором величина - логарифм априорной вероятности числа. Она

является наибольшей среди всех мыслимых разновидностей сложности (теорема 2). Эта величина, таким образом превышает обычную колмогоровскую сложность, но как показывает теорема 3, не более чем на логарифм этой сложности.

Во второй главе с алгоритмической точки зрения изучаются случайные процессы. Основными результатами главы является построение универсальной полувычислимой меры, изучение ее свойств, связи со сложностью и некоторые применения полученной теории.

Вначале рассматриваются вычислимые меры - распределения вероятностей на пространстве бесконечных двоичных последовательностей. Регулярные процессы (почти всюду определенные вычислимые операторы) не выводят из класса этих мер и устанавливают их эквивалентность. Однако применение к вычислимым мерам нерегулярных процессов (произвольных вычислимых операторов) порождает на выходе этих процессов распределение вероятностей, которое уже не обязательно будет вычислимым. Теорема 9 дает простой критерий того, может ли мера P быть получена таким образом. Эти меры называются полувычислимыми. Среди них существует максимальная, с точностью до мультипликативной константы (теорема 10). Она называется универсальной мерой. Логарифм этой меры будет оптимален уже с точностью до аддитивной константы и по своим алгоритмическим свойствам аналогичен сложности. Оказывается, что он и численно близок к сложности разрешения $KR(x)$ (хотя это совпадение только асимптотическое). А именно, теорема II утверждает, что

$$|KR(x) - (-\log_2 R\{\Gamma_x\})| \preceq 2\log_2 KR(x)$$

где $R\{\Gamma_x\}$ - универсальная мера множества последовательностей, начинающихся со слова x . Интересно отметить, что логарифм

универсальной меры вписывается в общую конструкцию V-мажоранту, развитую во введении и так же соотносится с логарифмом априорной вероятности числа (из теоремы 2), как сложность разрешения $KR(x)$ со сложностью $K(x)$. Теория полувычислимых мер оказывается полезной для решения ряда вопросов. Два из ее применений вошли в диссертацию. Это, во-первых, теорема 17 (она относится к последней главе и о ней будет еще речь впереди) и, во-вторых, последний параграф второй главы "Вероятностные машины". В этом параграфе аппарат полувычислимых мер применяется к изучению возможностей вероятностных машин (алгоритмов, использующих датчик случайных чисел). В известной работе Шеннона и других было показано, что такие машины не могут решать задач, неразрешимых детерминированными машинами, если эти задачи имеют единственное решение. Интерес к этим машинам возродился после того, как Я.М.Барздинь в работе [5] привел пример интересной задачи, неразрешимой детерминированными машинами, но разрешимой с помощью вероятностной машины. (Разумеется решение этой задачи не единственно).

В диссертации рассматривается вопрос о количестве обращений к датчику случайных чисел, необходимом для решения произвольной задачи. Очевидно, что даже машина, использующая вместо датчика случайных чисел специально подобранный для задачи оракул любой природы, не может обратиться к нему меньшее число раз, чем сложность требуемого результата. Но, по теореме 13, уже это количество обращений оказывается достаточным, даже для машины с обычным вероятностным оракулом (если такие машины в принципе способны с положительной вероятностью решить данную задачу). Отсюда, в частности, вытекает, что любая вероятностная машина может быть заменена слабо табличной. В кон-

це параграфа приведены два результата о невозможности получения на вероятностной машине быстрорастущих последовательностей.

Третья глава посвящена алгоритмическому подходу к теории информации. А.Н.Колмогоров определяет количество информации в слове y о слове x ($I(y:x)$) как разность между сложностью x ($K(x)$) и сложностью x при известном y ($K(x|y)$). Оказывается, что для этой величины нарушается свойство коммутативности, хорошо известное для "классической" вероятностной информации. Стояла проблема, имеет ли место это свойство приближенно. Она была независимо решена А.Н.Колмогоровым и автором настоящей диссертации. А именно, теорема I6 утверждает, что

$$|I(x:y) - I(y:x)| \leqslant c \log K(x,y)$$

Последний результат настоящей диссертации (теорема I7) составляет положительное решение проблемы (постановка которой принадлежит Дж.Т.Шварцу) о совпадении энтропии произвольной динамической системы (стационарного случайного процесса) с удельной сложностью почти всех ее траекторий. В случае процесса независимых испытаний этот факт установил еще А.Н.Колмогоров.

Результаты диссертации докладывались на симпозиуме по алгоритмическим сложностям, на симпозиуме - школе по основаниям математики, на вероятностной секции Московского математического общества, на семинаре по конструктивной математике А.А.Маркова, семинаре лаборатории статистических методов МГУ и ряде других семинаров. Опубликованы они в обзорной статье [6] с указанием авторства.

Я испытываю глубокую благодарность к моему научному руководителю А.Н.Колмогорову к А.К.Звонкину, оказавшим большую помощь в изложении результатов, а также к В.Н.Агафонову, Я.М. Барздиню, Р.А.Добрушину, А.Г.Драгалину, М.И.Кановичу, А.Н.Колодию, Мартин-Лефу П., Л.Б.Медведовскому, Н.В.Петри, А.Б.Сосинскому, В.А.Успенскому, Дж.Шварцу и всем участникам семинара А.А.Маркова за обсуждение.

ЛИТЕРАТУРА

I. В.Н.Агафонов, Об алгоритмах, частоте и случайности, Кандидатская диссертация, Новосибирск, I970.

2. Я.М.Барздинь, Сложность и частотное решение некоторых алгоритмически неразрешимых массовых проблем, препринт, I970.

3. Я.М.Барздинь, Сложность программ, распознающих принадлежность натуральных чисел, не превышающих n, рекурсивно перечислимому множеству, ДАН I82 (I968), I249-I252.

4. Я.М.Барздинь, О частотном решении алгоритмически неразрешимых массовых проблем, ДАН I9I (I970), 967-970.

5. Я.М.Барздинь, О вычислимости на вероятностных машинах, ДАН I89 (I969), 699-702.

6. А.К.Звонкин и Л.А.Левин, Сложность конечных объектов и обоснование понятий информации и случайности с помощью теории алгоритмов, УМН, I970, вып. 6, стр. 85-I27.

7. М.И.Канович, О сложности перечисления и разрешения предикатов, ДАН I90 (I970), 23-26.

8. М.И.Канович, Н.В.Петри, Некоторые теоремы о сложности нормальных алгорифмов и вычислений, ДАН I84 (I969), I275-I276.

9. М.И.Канович, О сложности разрешения алгоритмов, ДАН

186 (1969), 1008-1009.

10. А.Н.Колмогоров, Три подхода к определению понятия "количество информации", Проблемы передачи информации 1:1 (1965), 3-7.

11. А.Н.Колмогоров, К логическим основам теории информации и теории вероятностей, Проблемы передачи информации 5:3 (1969), 3-7.

12. А.Н.Колмогоров, Несколько теорем об алгоритмической энтропии и алгоритмическом количестве информации, УМН 23:2(1968), 201.

13. К.де Леу, Э.Ф.Мур, К.Шеннон, Н.Шапиро, Вычислимость на вероятностных машинах, Автоматы (сб.переводов), М.,ИЛ,1956.

14. Р.Б.Маранджан, О некоторых свойствах асимптотически оптимальных рекурсивных функций, Изв. АН Арм.ССР 4:1 (1969), 3-22.

15. А.А.Марков, О нормальных алгорифмах, связанных с вычислением булевских функций и предикатов, Изв. АН, сер.матем., 31 (1967), 161-208.

16. А.А.Марков, О нормальных алгорифмах, вычисляющих булевы функции, ДАН 157 (1964), 262-264.

17. П.Мартин-Леф, О колебании сложности бесконечных двоичных последовательностей, препринт, 1970.

18. П.Мартин-Леф, О понятии случайной последовательности, Теория вероятн. и ее примен. 11 (1966), 198-200.

19. Н.В.Петри, Сложность алгорифмов и время их работы, ДАН 186 (1969), 30-31.

20. Н.В.Петри, Об алгорифмах, связанных с предикатами и булевыми функциями, ДАН 185 (1969), 37-39.

21. Б.А.Трахтенброт, Сложность алгоритмов и вычислений,

Новосибирск, 1967.

22. С.В.Яблонский, Об алгоритмических трудностях синтеза минимальных схем, Проблемы кибернетики, 2, 1959, 75-121.

23. G.H.Chaitin, On the length of programs for computing finite binary sequences, I, II, Journ. Assoc. Comp. Mach. 13 (1966), 547-570; 15 (1968)

24. A.Kolmogoroff, Logical basis for information theory and probability theory, IEEE Trans., IT-14 (1968), 662-664

25. D.W.Loveland, A variant of the Kolmogorov conception of complexity, Inform. Control 15 (1968), 510-527

26. Mann I. Probabilistic recursive functions, J. Symbolic Logic 31 (1966), 698

27. P.Martin-Löf, The definition of random sequenses, Inform. Control 9 (1966), 602-619

28. P.Martin-Löf, Algorithms and random sequences, University of Erlangen, 1966

29. P.K.Schnorr, Eine neue Charakterisierung der Zufälligkeit von Folgen, preprint, 1970

30. R. J.Solomonoff, A formal theory of inductive inference, Inform. Control 7 (1964), 1-22

Подписано к печати 9/XII-1971 г. МН 16005
Формат бумаги 60х84 1/16. Объем 0,41 п.л. 0,37 уч.-изд.л.
Заказ 597 Тираж 180 экз.

Отпечатано на ротапринте Института математики СО АН СССР
Новосибирск, 90